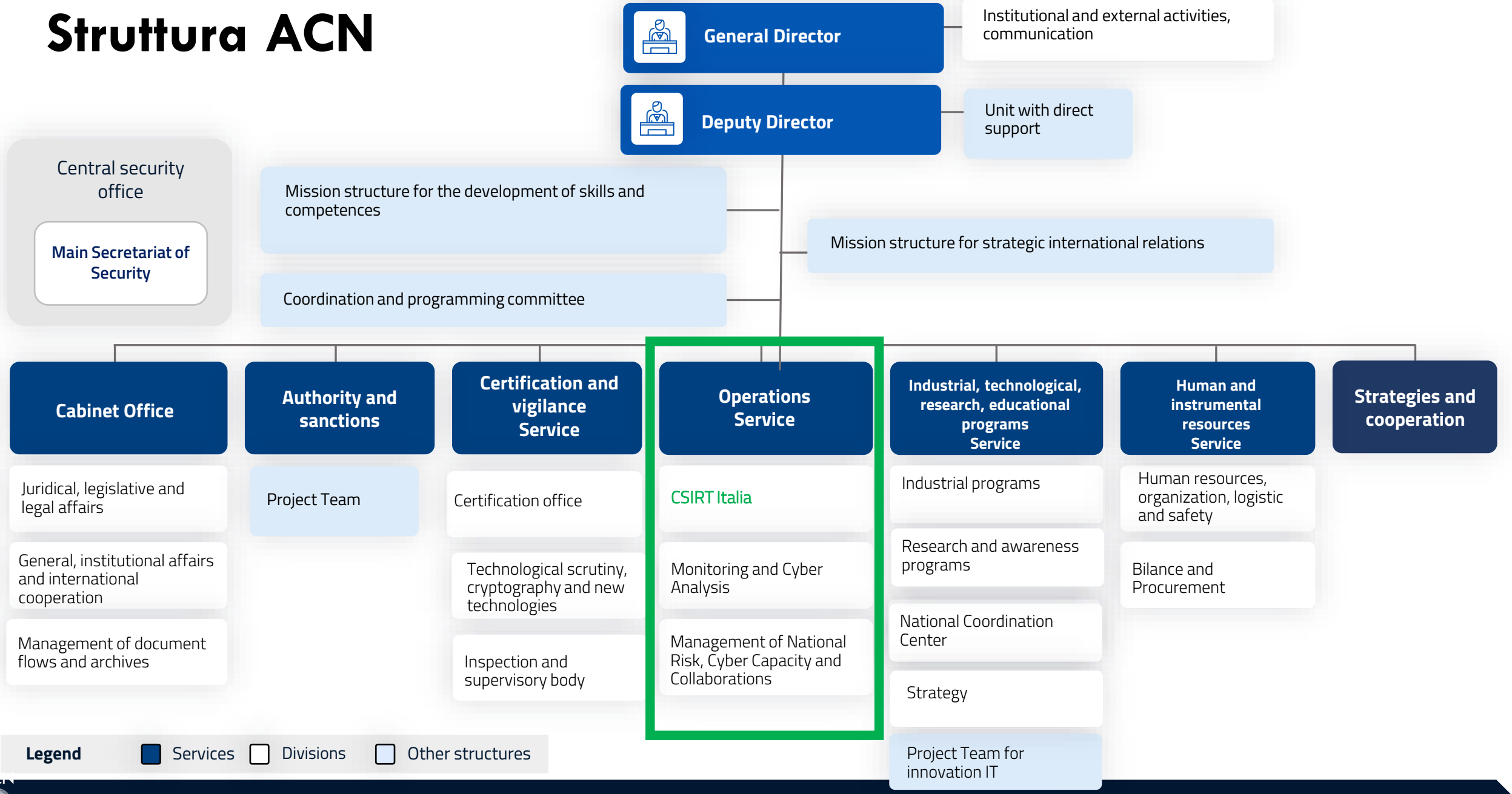
La gestione degli incidenti cyber

Il ruolo dello CSIRT Italia, indicazioni utili per le PA, la gestione degli incidenti

Roma, 22.04.2024

D.L. 14 giugno 2021, n. 82 - Architettura Nazionale Cyber

Struttura ACN



Servizio Operazioni - Mission e Articolazione

Il Servizio Operazioni è la **struttura operativa** dell'Agenzia incaricata delle attività di prevenzione, monitoraggio, rilevamento, analisi e risposta per prevenire e gestire eventi di natura cibernetica, all'interno della quale opera lo **CSIRT Italia** istituito dal D.lgs. n. 65 del 2018 attuativo della Direttiva NIS.

Per assicurare lo svolgimento delle funzioni operative, il servizio svolge **compiti di natura *proattiva*** (monitoraggio, cyber threat intelligence, analisi specialistica sulle minacce ed early warning su eventi d'interesse), **di *natura reattiva*** (incident response, analisi malware, digital forensics ed analisi "post-mortem") e **servizi di *risk management & governace*.**

CSIRT: Computer Security Incident Response Team
MAC: Monitoraggio ed Analisi Cyber
GRICC: Gestione Rischio Nazionale, Capacità Cyber e Collaborazioni

Sintesi servizi erogati

CSIRT Italia

SERVIZI REATTIVI

- INCIDENT HANDLING SUPPORT 24/7
- REMEDIATION PLAN DEFINITION SUPPORT
- MALWARE & SUSPICIOUS ARTIFACT ANALYSIS
- DFIR TEAM (DEPLOYABLE IF NEEDED)

SERVIZI PROATTIVI

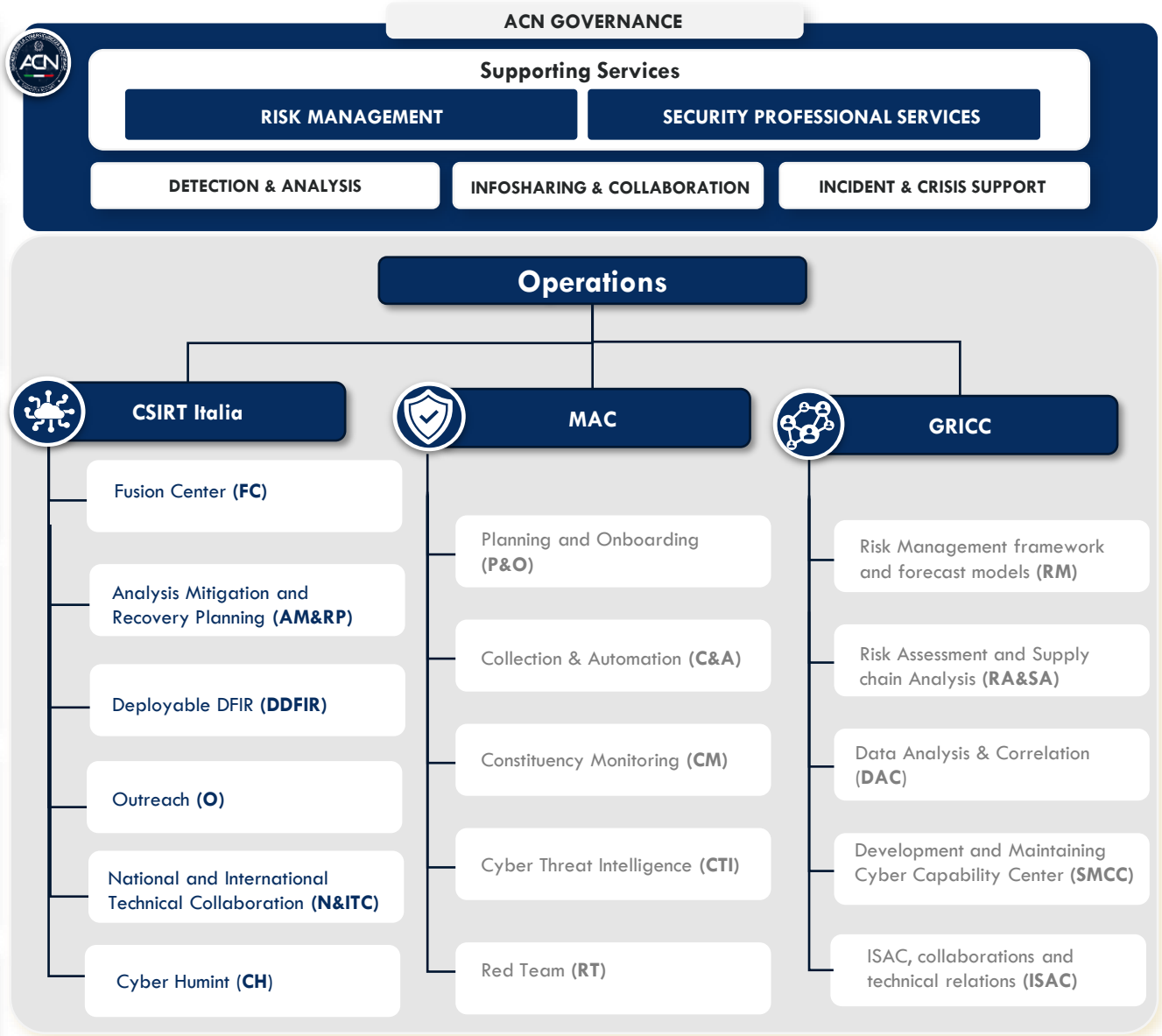
- EXPOSED ATTACK SURFACE MONITORING
- ACTORS, CAMPAIGNS & VULNERABILITY MONITORING
- EXPERT ANALYSIS ON CYBER THREATS
- EARLY WARNING ON EVENTS OF NATIONAL RELEVANCE

GESTIONE RISCHIO & GOVERNANCE

- INCIDENT SYSTEMIC IMPACT EVALUATION
- RISK MANAGEMENT
- FORECAST ANALYSIS AND THREAT TRENDS
- ACCREDITATION & CERTIFICATION

Modello Organizzativo

Fusion Center (FC)	Responsabile dell'analisi di primo livello sulle notifiche fornite dalla Constituency e dai Partner ai sensi delle normative nazionali e internazionali. Le attività sono principalmente focalizzate sull'acquisizione, validazione, classificazione e triage delle segnalazioni al fine di affidare in modo efficace la propria risposta agli organi competenti interni e/o esterni ad ACN.
Analysis Mitigation and Recovery Planning (AM&RP)	Responsabile dell'analisi di secondo livello a seguito dell'incarico di FC. Le sue attività si concentrano principalmente sugli stakeholder di livello 3 (o supporto di livello 4) e si basano su indagini, risposta, mitigazione e supporto al ripristino. AM&RP sarà coinvolto anche nella fornitura di altre capacità all'interno di CSIRT; l'arricchimento della base di conoscenza; gestione agli eventi cyber di natura critica.
Deployable DFIR (DDFIR)	Responsabile dell'analisi di livello due e tre in seguito all'assegnazione di FC o all'escalation degli incidenti assegnati ad AM&RP. Le sue attività si basano su indagine, risposta, mitigazione, analisi forense digitale su prove e artefatti e supporto al ripristino degli incidenti segnalati dalle parti interessate di livello 4 e potrebbero essere fornite sia in remoto che in loco.
Outreach	Gestisce le procedure di comunicazione dal CSIRT alla constituency; diffonde bollettini, alert e vulnerabilità; trasmette allerte e notifiche alle altre amministrazioni interessate; pubblicazioni sulle migliori pratiche e lezioni apprese relative agli incidenti gestiti; custodisce l'elenco aggiornato dei contatti del CSIRT e della constituency e fa attività di awareness alla sicurezza informatica.
National and International Technical Collaboration (N&ITC)	Responsabile dello sviluppo e dell'aggiornamento delle procedure operative CSIRT in linea con gli standard internazionali; coordinamento e organizzazione della partecipazione ad esercitazioni di gestione di eventi/crisi con profili di cybersecurity; relazioni tecniche CSIRT; supporto alla risposta del Cybersecurity Core alla crisi cyber da parte delle amministrazioni e degli operatori privati coinvolti.
Cyber Humint (CH)	Responsabile dell'acquisizione di precursori e informazioni relative agli incidenti attraverso l'indagine di fonti OSINT e CLOSINT come il deep dark web, social network, punti di informazione specializzati, ecc.



Constituency

I servizi sono forniti ai settori PUBBLICO e PRIVATO

per livelli 0 – 1 – 2 – 3 - 4 (critico)

Società identificate quali NIS, OSE, inserite in Perimetro e/o Telco (4), Regioni, città metropolitane

Ministeri CIC, P.A. centrali, Regioni, città metropolitane, P.A. identificate OSE, P.A. inserite in Perimetro (4)

Organizzazioni di grande entità & altre P.A. (non critiche, ma operanti nei settori Perimetro, NIS e Telco - 3)

Organizzazioni di media entità (operanti nei settori Perimetro, NIS e Telco - 2)

Altre P.A. & Organizzazioni di piccola entità (operanti nei settori Perimetro, NIS e Telco - 1)

Altre organizzazioni private non operanti in settori Perimetro, NIS e Telco (0)

PMI e privati best effort / emergenza

Compiti e servizi ACN – CSIRT Italia

- Punto unico ricezione allarmi e notifiche Perimetro – NIS – OSE/FSD
- Monitoraggio incidenti H24 7/7
- Produzione Alert – Bollettini – Approfondimenti
- Comunicazioni P2P - Massive
- Collaborazione CNAIPIC / PNAA
- Interventi a supporto on-site e off-site in caso di incidenti & Team DFIR
- Partecipazione CSIRT Network / Rete CSIRT Regionali
- Collaborazioni con Accademia, settore Pubblico e Privato a livello nazionale e internazionale
- Supporto a CIC – CISR – NISP
- Raccordo con CVCN
- Partecipazione ad esercitazioni cyber nazionali ed internazionali (NATO – UE – G7)
- Attività di cyber awareness e promozione best practice

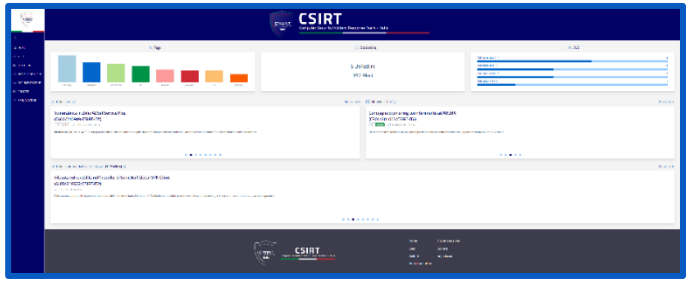
Portali e caselle istituzionali

Portale Pubblico

- **Consultabile liberamente** all'indirizzo **https://www.csirt.gov.it**
- Condivisione **Alert, bollettini, monografie** e **Indicatori** relativi a minacce cyber
- Contenuti e informazioni ad accesso pubblico con **TLP WHITE**

Portale Collaboration

- Dedicato ai **soggetti NIS, PNSC** ed altri di interesse
- Contenuti ad accesso controllato con **TLP GREEN, AMBER, RED**
- Accreditamento tramite richiesta del soggetto (info@csirt.gov.it)



Caselle di posta istituzionali

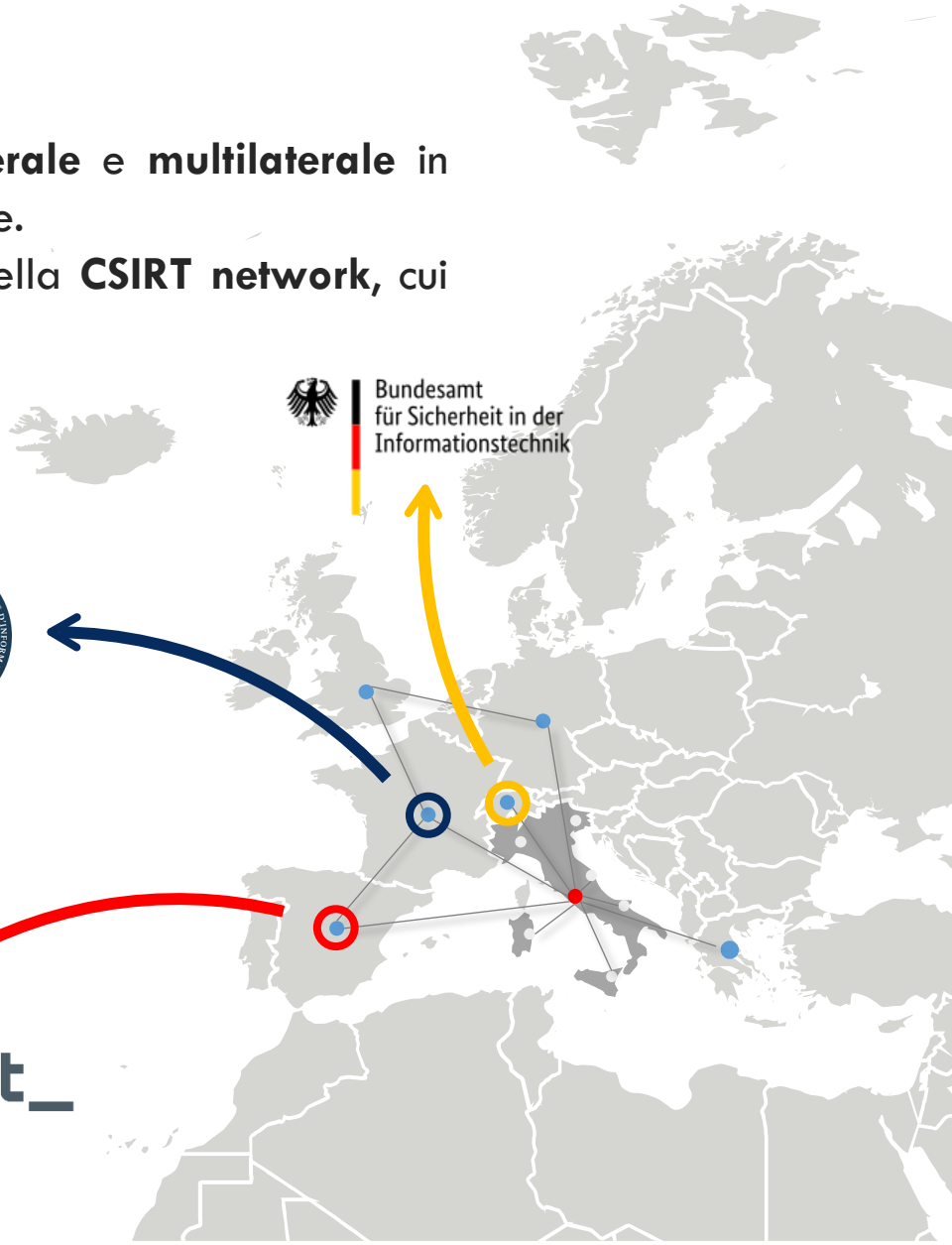
- Segnalazioni relative a **eventi** di **cybersicurezza**
- Comunicazioni punto-punto relative a **specifiche evidenze**
- **Interlocuzioni** di **natura tecnica** in materia di cybersicurezza

Posta elettronica ordinaria:
info@csirt.gov.it

Posta elettronica certificata:
csirt@pec.acn.gov.it

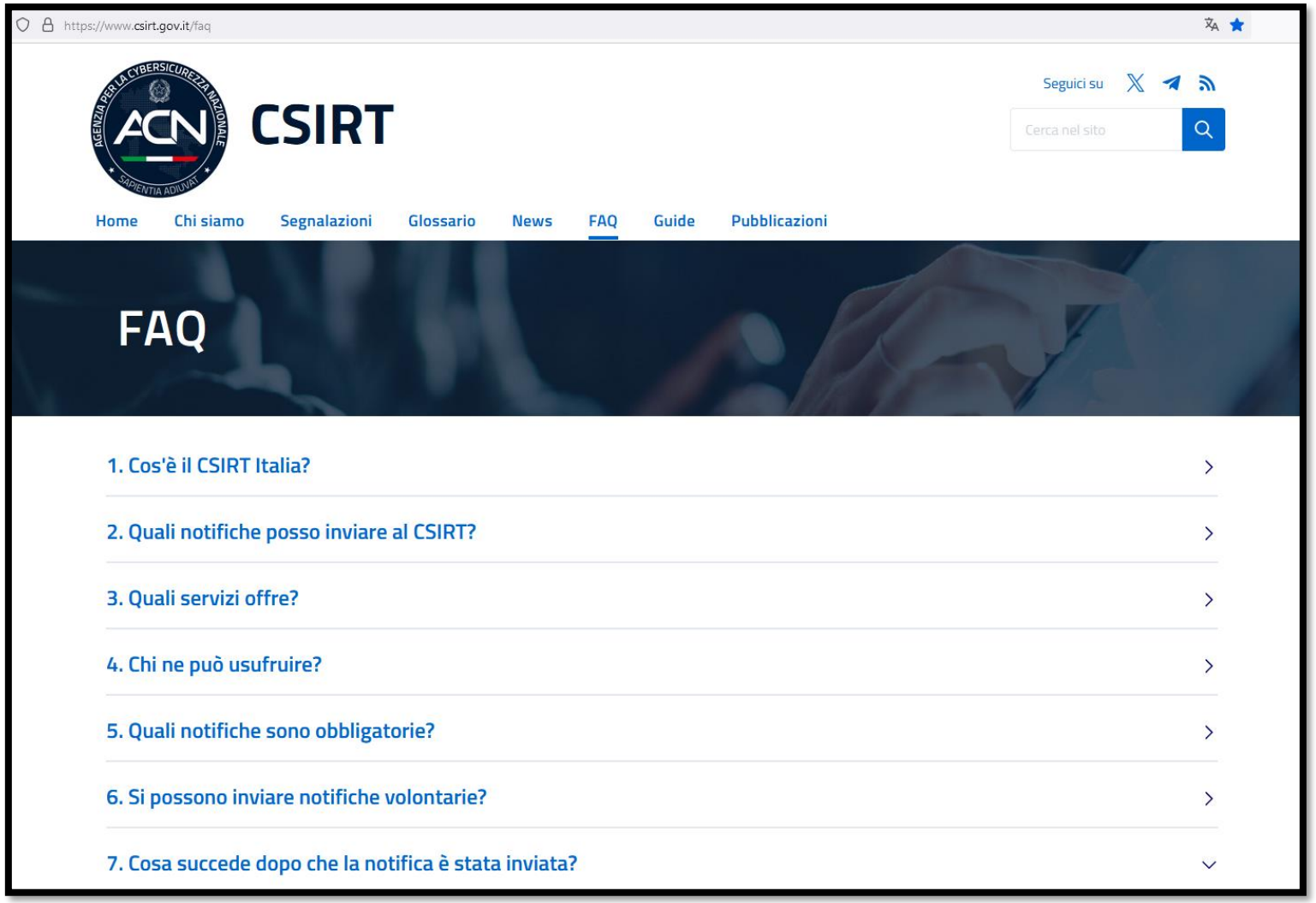
Collaborazioni Internazionali

Lo CSIRT Italia collabora con numerose realtà straniere su base **bilaterale** e **multilaterale** in tema di information-sharing, early warning e condivisione di best practice.
Un circuito di scambio multilaterale particolarmente efficace è quello della **CSIRT network,** cui partecipano tutti i Stati membri dell'UE.



Ulteriori informazioni

www.csirt.gov.it/faq



Obiettivi dell' Incident Response

Analisi

- Determinare il vettore di attacco
- Determinare i tool ed il malware utilizzato
- Identificare i sistemi compromessi e le modalità di compromissione
- Determinare la profondità della compromissione e eventuali impatti sulla confidenzialità dei dati gestiti
- Determinare se l'incidente è ancora in corso
- Identificare la timeline dell'incidente

Ripristino

Utilizzare le informazioni raccolte per definire ed eseguire il piano di rimedio

Non agire troppo in fretta

Neanche troppo lento però…

Takeaway

Fattori di rischio

- Iniziare il processo di remediation senza avere abbastanza elementi espone a maggiori rischi
- L'attaccante potrebbe identificare le azioni di remediation ed intensificare le attività di persistenza o effettuare azioni distruttive
- Ripristinare immediatamente i sistemi senza le corrette informazioni può generare impatti imprevisti ed esporre l'infrastruttura a maggiori rischi
- Effettuare attività invasive o di ripristino immediato potrebbe portare alla distruzione di evidenze fondamentali

Non nasconderti

Takeaway

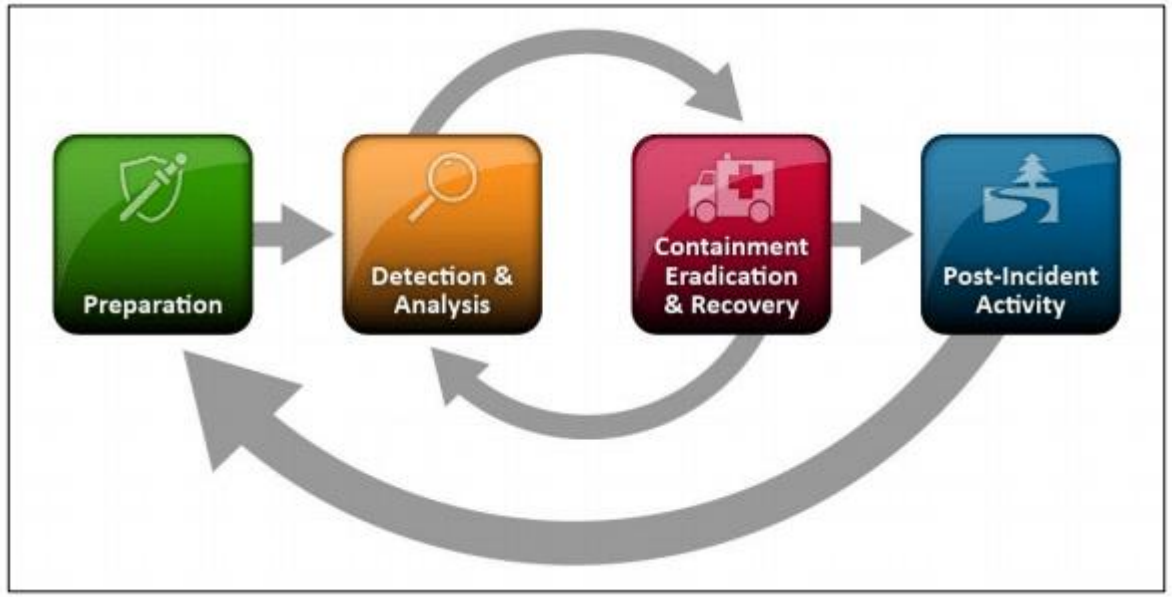
Attività di comunicazione

- Provare a nascondere o minimizzare un incidente può comportare un maggiore impatto sia dal punto di vista mediatico sia dal punto di vista operativo
- Segnalare un incidente agli organi preposti oltre a scongiurare la possibilità di incappare in regimi sanzionatori consente di ottenere supporto e di proteggere la comunità nazionale
- Una comunicazione efficace interna ed esterna all'organizzazione consente di prevenire ulteriori danni d'immagine di agevolare le attività del team di risposta

Segui un approccio strutturato

Takeaway

Processo di Incident Response



Conosci i tuoi sistemi

Takeaway

Preparation

- Mantenere aggiornato l'asset management
- Categorizzare i sistemi ed i dati utilizzati in base alle loro funzioni e criticità
- Identificare e mantenere una lista degli stakeholder (ruoli/responsabilità/contatti)
- Formare il personale a tutti i livelli sui rischi cibernetici sulle buone pratiche da adottare e sulle procedure di risposta agli incidenti informatici

Ottieni visibilità e approfondisci ogni evento

Takeaway

Detection & Analysis

- Mantenere la più ampia visibilità su tutto l'ambiente da proteggere (EDR/XDR/SIEM/SOAR/TI…)
- Definire una baseline di funzionamento dei propri sistemi
- Monitorare costantemente il proprio ambiente alla ricerca di anomalie
- Prioritizzare l'analisi delle anomalie rilevate in base alla categorizzazione degli asset
- Approfondire qualsiasi comportamento, informazione o segnalazione ricevuta che possa rappresentare un precursore o un indicatore di incidente

Observe, Orient, Decide, Act

Takeaway

Containment Eradication & Recovery

- Limitare le capacità dell'attaccante per prevenire ulteriori impatti mantenendo attive le funzioni essenziali
- Identificare e bloccare i canali di comando e controllo dell'attaccante
- Identificare e rimediare le ulteriori vie d'accesso presenti nella rete (es. vulnerabilità misconfigurazione utenze dormienti)
- Identificare e «bonificare» tutti gli asset compromessi/utilizzati dall'attaccante
- Ripristinare tutti i servizi affetti prendendo tutte le misure necessarie per evitarne la recompromissione
- Documentare tutte le evidenze rilevate e le attività effettuate in dettaglio

Un incidente è un occasione per migliorare

Takeaway

Post-incident Activity

- Valutare l'efficacia dei processi di gestione dell'incidente implementati e revisionarli in base all'esperienza acquisita
- Identificare i gap capacitivi e di processo che hanno facilitato/consentito l'incidente
- Avviare un processo continuo di revisione della postura e delle procedure operative adottate

GRAZIE


AGENZIA PER LA CYBERSICUREZZA NAZIONALE
ACN
SAPIENTIA ADIUVAT